UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 08/03/2010

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER
ZECHER, CORDELIA P K

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
08/03/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/752,420	ROSE ET AL.	
	Examiner	Art Unit	
	Cordelia Zecher	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-24,26-28,50,51 and 53-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 28, 2010 has been entered.

Response to Arguments

2. Applicant's arguments, see Remarks, filed June 28, 2010, with respect to the 101 rejection have been fully considered and are persuasive. The rejection of claims 14 – 21 has been withdrawn.

3. Applicant's arguments with respect to claims 1 – 3, 5 - 24, 26 - 28, 50, 51 and 53 - 68 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claims 67 and 68 objected to because of the following informalities: The claims refer to the "method of claim 65". However, claim 65 is a machine readable medium claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 14 – 21 and 61 – 64 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim element "means for storing", “means for creating”, etc. are means plus function limitations that invoke 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function.

7. Applicant is required to:

(a) Amend the claim so that the claim limitation will no longer be a means (or step) plus function limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend tile written description of the specification such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

8. If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant is required to clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the

claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform the claimed function. F& more information, see 37 CFR 1.75(d) aid MPEP 2lsi and 608.01(0).

9. For a computer-implemented means-plus-function claim limitation that invokes 35 U.S.C. 112, sixth paragraph, the corresponding structure is required to be more than simply a general purpose computer or microprocessor. The corresponding structure for a computer-implemented function must include the algorithm as well as the general purpose computer or microprocessor.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 22 – 24, 26 – 28, and 65 – 68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. there is no definition in the specification to define a machine readable medium. To those of ordinary skill in the art, the term machine readable medium includes signals. Signals do not fall into one of the four statutory categories of invention. Therefore the claims are non-statutory. To

overcome the ordinary meaning in the art, a definition prohibiting signals or a negative limitation (medium excluding signals, or non-transitory medium) needs to occur.

Claim Rejections - 35 USC § 103

12. Claims 1 – 3, 5 – 9, 11 – 14, 16 – 24, 26 – 28, 50, 51, and 53 – 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan et al's US Patent 6,782,103 B1, and further in view of Sudia US Patent 6,009,177.

13. Referring to claims 1, 14 and 22, Arthan teaches:

a. Creating a first private key and corresponding public key (column 4, lines 25-30).

b. Creating a second private key associated with the first private key and creating a second public key corresponding to the second private key (column 4, lines 25-30).

c. Outputting the second private key while retaining the first private key (column 4, lines 30-32) such that the first private key is inaccessible (column 5, lines 30-35).

d. Transmitting the first public key and the second public key to a verifier device (column 4, lines 18-20).

e. Using the first private key for authentication (column 4, lines 15-16).

14. Arthan fails to teach a wireless network, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more

than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

15. Referring to claims 2 and 23, Sudia teaches:

f. Creating at least two shares of the second private key at the device (column 18, lines 12-14).

g. Outputting each share to a different entity (column 18, lines 37-39).

16. Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

17. Referring to claims 3, 16, and 24, Arthan teaches using the second private key independent of the first private key for authentication (column 4, lines 20-23). Sudia

teaches re-creating the private key using at least some shares of the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

18. Referring to claims 5 and 17, Arthan teaches:

h. Creating a third private key associated with the second private key, and creating a third public key corresponding to the third private key (column 5, lines 12-14).

i. Outputting the third public key to the verifier (column 5, lines 12-14).

19. Referring to claim 6, Arthan teaches:

j. Outputting the third private key (column 4, lines 30-32).

k. Using the third private key for authentication (column 4, lines 20-23).

20. Sudia teaches:

l. Outputting the key as a plurality of shares such that it can be recreated (column 18, lines 12-14).

m. Recreating the private key using at least some of the plurality of shares (column 31, lines 45-55).

21. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

22. Referring to claim 7, Arthan teaches that the second private and public keys are created independently from the first private and public keys (column 4, lines 25-26).

23. Referring to claims 8 and 18, Arthan teaches:

n. Creating a third private key associated with the second key and creating a third public key corresponding to the third private key (column 5, lines 12-14).

o. Creating a fourth private key associated with the third private key and creating a fourth public key corresponding to the fourth private key (column 4, lines 25-30).

p. Outputting the third and fourth public keys (column 4, lines 18-20).

24. Arthan fails to teach outputting the fourth private key once such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

25. Referring to claim 9, Arthan teaches:

q. Disabling use of the second private key for authentication (column 4, lines 20-23).

r. Using the third private key for authentication (column 4, lines 20-23).

s. Accessing the fourth private key (column 4, lines 20-23).

t. Using the fourth private key for authentication (column 4, lines 20-23).

26. Arthan fails to teach recreating the fourth private key. Sudia teaches re-creating the private key using the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

27. Referring to claims 11, 19, and 26, Arthan discloses:

u. Receiving a first public key (column 4, lines 18-20).

v. Receiving a second public key, the second public key associated with the first public key (column 4, lines 18-20), wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to the first public key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

w. Using the first public key for authentication (column 5, lines 12-14).

x. Using the second public key for authentication if the first public key fails (column 5, lines 12-14).

28. Arthan fails to teach a mobile user device, or distributing a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

29. Referring to claims 12, 20 and 27, Arthan teaches receiving a third public key from the device, the third public key associated with the second public key (column 5, lines 12-14), if the first public key fails and the second key results in successful authentication (column 4, lines 20-23).

30. Referring to claims 13, 21, and 28, Arthan teaches a third public key and a fourth public key from the device (column 5, lines 12-14), if the first public key fails and if the second public key results in a successful authentication, wherein the third and fourth public keys are associated with the second key (column 4, lines 20-26).

31. Referring to claim 50, Arthan teaches:

y. A processor configured to generate a first private key and corresponding first public key, generate a second private key associated with the first private key and to create a second public key corresponding to the second private key (column 4, lines 25-30).

z. A storage medium coupled to the processor to store the first private key (column 2, lines 48-50).

aa. A transmitter to output the second private key such that it can be used when there is no access to the first private key wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 25-32).

bb. Output the first public key and the second public key to a verifier device (column 4, lines 18-20).

cc. Wherein the processor uses the first private key for authentication of the device (column 4, lines 12-14).

32. Arthan fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks communications include cell phones (column 26, line 65). Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to

modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

33. Referring to claim 51, Arthan teaches:

dd. A receiver configured to receive a first public key from a device and receiving a second public key from the device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that can be used when there is no access to a first private key corresponding to a first public key, wherein the first private key is disabled when the second private key is recreated and used for authentication (column 4, lines 15-30).

ee. A storage medium coupled to the receiver configured to store the first and second public keys (column 4, lines 18-20).

ff. A processor coupled to the receiver and the storage medium, the processor configured to use the first public key for authentication, the processor configured to use the second public key for authentication if the first public key fails (column 4, lines 18-20).

34. Arthan fails to teach a wirelessly outputting a plurality of shares of the private key to a plurality of different entities such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Sudia also discloses that the networks

communications include cell phones (column 26, line 65). Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

35. Referring to claims 53 – 56, Arthan teaches the second private key is removed from the user device upon transmission of the second private key (column 4, lines 30-32).

36. Arthan fails to teach a wirelessly transmission of a plurality of shares of the private key. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

37. Referring to claims 57, 61 and 65, Arthan teaches:

gg. Retrieving a second private key at a mobile user device that has no access to a first private key associated with the second private key (column 5, lines 12-14).

hh. Creating a third private key and a corresponding third public key (column 5, lines 12-14).

ii. Using the second private key for authentication (column 4, lines 20-23).

38. Sudia teaches re-creating the private key using at least some shares of the plurality of shares (column 31, lines 45-55). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

39. Referring to claim 58, 62 and 66, Sudia teaches recreating the second private key at a mobile user device different from a mobile user device that created the first private key and second private key (column 7, lines 8-11). At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

40. Referring to claims 59, 63, and 67, Arthan teaches:

jj. Outputting the third private key while retaining the second private key (column 4, lines 30-32).

kk. Transmitting the third public key to the verifier device (column 4, lines 18-20).

41. Sudia teaches outputting the key as a plurality of shares such that it can be recreated (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

42. Referring to claims 60, 64, and 68, Arthan teaches:

ll. Creating a fourth private key and a corresponding fourth public key (column 4, lines 25-30).

mm. Outputting the fourth private key while retaining the third private key (4, lines 30-32).

nn. Outputting the third and fourth public keys (column 4, lines 18-20).

43. Arthan fails to teach outputting the fourth private key as a plurality of shares such that it can be recreated. However, Sudia teaches breaking the key into several key splits, and escrowing the key with more than one escrow agent (column 18, lines 12-14). The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

44. Claims 10 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan in view of Sudia as applied above, and further in view of Official Notice. Referring to claim 10, Arthan in view of Sudia discloses all the limitations of the parent claim. Arthan in view of Sudia does not explicitly disclose preventing retransmission of the second private key. However, Arthan teaches that the key is encrypted and stored securely (column 5, lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

45. Referring to claim 15, Sudia teaches:

oo. Creating at least two shares of the second private key at the device (column 18, lines 12-14).

pp. Outputting each share to a different entity (column 18, lines 37-39).

46. Arthan and Sudia are analogous art because they are from the same field of endeavor, encrypted communications. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Arthan and Sudia before him or her, to modify the system of Arthan to include the wireless communication and private key distribution of Sudia. The suggestion/motivation for doing so would have been that it is desirable to have the key split among multiple key escrow agents to enhance user and public trust in the system (column 20, lines 66-column 21, line 4).

47. Arthan in view of Sudia does not explicitly disclose subsequent outputting of the key is prevented. However, Arthan teaches that the key is encrypted and stored securely (column 5, lines 26-28) and that it should be held securely after generation (column 4, lines 30-31). The examiner takes official notice that it would have been obvious, to one of ordinary skill in the art at the time of invention, to prevent retransmission of the key since keeping the key stored securely is important and that retransmission would expose the key to more vulnerabilities.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Zecher whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/C. Z./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432